UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/685,882	10/15/2003	Vincent J. Zimmer	20002/17849	5946

34431 7590 01/08/2008

HANLEY, FLIGHT & ZIMMERMAN, LLC
150 S. WACKER DRIVE
SUITE 2100
CHICAGO, IL 60606

EXAMINER	
MORAN, RANDAL D	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
01/08/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/685,882	ZIMMER ET AL.	
	Examiner	Art Unit	
	Randal D. Moran	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-32 are pending.

2. This Office action in response to amendment filed 10/22/2007.

3. Below, Examiner has pointed out particular references contained in the prior art(s) of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claims, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully each reference in its entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. **Claims 1, 3, 5, 6, 8, 10-12, 15, 17-21, and 25-28, 30-32** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Rawson (US 6,182,223),** hereafter "Rawson" in view of **Mitchem, T.; Lu, R.; O'Brien, R; Using Kernel Hypervisors to Secure Applications, IEEE, Dec. 1997 Page(s): 175-181**, hereafter "Mitchem", in view of **Lettvin (US 5,559,960),** hereafter "Lettvin".

3. Considering **Claims 1, 8, 15, and 23,** Rawson discloses a method to provide network traffic support and physical security support (abstract) comprising: identifying at least one of a network traffic intrusion event and a physical security intrusion event with the VMM (column 6- lines 4-20); and implementing at least one of a network traffic support and a physical security support in response to the at least one of the network traffic intrusion event and the physical security intrusion event (column 4- lines 12-27).

Rawson does not explicitly disclose initializing a virtual machine monitor (VMM) in a processor system during a pre-boot phase.

Mitchem discloses initializing a virtual machine monitor (p. 179- 3.2- Client Kernel Hypervisors, ¶ 1-2).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Rawson by initializing the VMM as taught by Mitchem in order to protect a user, browsing on the internet, from downloading and executing malicious active content that might damage the user's system (Mitchem- p. 179- 3.2 Client Hypervisors, ¶ 2).

The combination of Rawson and Mitchem does not explicitly disclose the VMM is initialized during a pre-boot phase.

Lettvin discloses initializing a virtual machine monitor (VMM) in a processor system during a pre-boot phase (column 7-lines 23-67, column 8- lines 1-17, Fig. 3).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination of Rawson and Mitchem by initializing the VMM during a pre-boot phase as taught by Lettvin to provide a startup disk that causes the computer to automatically execute anti-virus software each time the computer starts from the disk, i.e., during bootstrap, so as to detect bootstrap time viruses before or after they have executed and implanted themselves in the system (Lettvin- column 2- lines 56-61).

4. Considering **Claims 3, 10, 17, 18, 25, and 26,** the combination discloses identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting opening of a chassis associated of the processor system via a chassis intrusion switch (Rawson- column 3- lines 4-11, column 6- lines 4-19).

5. Considering **Claims 5, 12, 20, and 28,** the combination discloses implementing the at least one of the network traffic support and the physical security support comprises disabling the processor system in response to identifying the physical security intrusion event (Rawson- column 4- lines 21-27).

6. Considering **Claim 6,** the combination discloses identifying a user authorization for the physical security intrusion event of the processor system (Rawson- column 4- lines 1-27).

7. Considering **Claim 14,** the combination discloses the machine readable medium comprises one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory, magnetic media, and optical media.
Rawson does disclose the machine readable medium comprises one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory,

magnetic media, and optical media (Lettvin- abstract, column 6- lines 15-39, Fig. 1).

8. Considering **Claim 21,** the combination discloses the data structure comprises a flash memory (Lettvin- abstract, column 2- lines 56-61).

9. Considering **Claim 30,** the combination discloses the VMM continuously identifies the at least one traffic intrusion and physical security intrusion event (Rawson- column 6- lines 4-20, Mitchem- p. 179- 3.2 Client Hypervisors, ¶ 2).

10. Considering **Claim 32,** the combination discloses initializing a plurality of virtual machines, wherein each of the plurality of virtual machines operates like a complete physical machine that can run its own operating system (Mitchem- Introduction, ¶ 1-2).

11. **Claims 2, 4, 7, 9, 11, 13, 16, 19, 22, 24, 27, 29, and 31** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Rawson, Lettvin, and Mitchem** in view of **Suuronen et al. (US 2003/0145228),** hereafter "Suuronen".

12. Considering **Claims 2, 9, 16, and 24,** the combination does not explicitly disclose identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting at least one of a

packet accessing a restricted port, a packet associated with a virus identifier, a SYN packet, and an alert standard format packet. Lettvin does suggest performing an integrity check on itself to ascertain whether it has bee damaged, e.g., by a virus attack, and announces the results of the self test (Lettvin- column 7- lines 23-27).

Suuronen discloses identifying the at least one of the network traffic intrusion event and the physical security intrusion event with the VMM comprises detecting at least one of a packet accessing a restricted port, a packet associated with a virus identifier, a SYN packet, and an alert standard format packet ([0005], [0010] lines 4-12, Fig. 1).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combination by identifying a virus identifier associated with network traffic as taught by Suuronen in order to provide a method of virus protection (Suuronen- abstract).

13. Considering **Claims 4, 11, 19, and 27,** the combination discloses implementing the at least one of the network traffic support and the physical security support comprises discarding a packet associated with network traffic in response to identifying the network traffic intrusion event (Suuronen- [0010] lines 4-12, Fig. 1).

14. Considering **Claims 7, 13, 22, and 29,** the combination discloses the processor system is associated with at least one of a private internal network and the Internet (Suuronen- Fig 2, Fig. 3).

15. Considering **Claim 31,** the combination discloses the VMM identifies both at least one of a network traffic intrusion event and at least one physical security intrusion event (Rawson- column 6- lines 4-20, Suuronen- abstract, Mitchem- p. 179, 3.2- Client Hypervisors, ¶ 2).

Response to Arguments

1. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

1. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Randal D. Moran whose telephone number is 571-270-1255. The examiner can normally be reached on M-F: 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Randal D. Moran
/RDM/

12/26/07

KIM VU
SUPERVISORY PATENT EXAMI
TECHNOLOGY CENTER 210